

# DESIGNS AND CODES IN AFFINE GEOMETRY

JENS ZUMBRÄGEL

**ABSTRACT.** Classical designs and their (projective)  $q$ -analogs can both be viewed as designs in matroids, using the matroid of all subsets of a set and the matroid of linearly independent subsets of a vector space, respectively. Another natural matroid is given by the point sets in general position of an affine space, leading to the concept of an affine design. Accordingly, a  $t$ -( $n, k, \lambda$ ) affine design of order  $q$  is a collection  $\mathcal{B}$  of  $(k-1)$ -dimensional spaces in the affine geometry  $\mathbf{A} = \text{AG}(n-1, q)$  such that each  $(t-1)$ -dimensional space in  $\mathbf{A}$  is contained in exactly  $\lambda$  spaces of  $\mathcal{B}$ . In the case  $\lambda = 1$ , as usual, one also refers to an affine Steiner system  $S(t, k, n)$ .

In this work we examine the relationship between the affine and the projective  $q$ -analogs of designs. The existence of affine Steiner systems with various parameters is shown, including the affine  $q$ -analog  $S(2, 3, 7)$  of the Fano plane. Moreover, we consider various distances in matroids and geometries, and we discuss the application of codes in affine geometry for error-control in a random network coding scenario.

## 1. INTRODUCTION

In recent years the  $q$ -analogs of combinatorial designs and Steiner systems enjoyed a considerable interest due to their relation with error-control in random network coding [11]. In this context a remarkable result has been the discovery of a nontrivial 2-ary  $S(2, 3, 13)$  Steiner system [3], whereas, perhaps surprisingly, no other  $q$ -analog of a Steiner system has been found since.

The present work aims to offer a new perspective on  $q$ -analog structures. While the  $q$ -analog designs studied so far can be seen as living in projective geometry, we propose to consider the setup of affine geometry. A suitable framework for both the “projective” and the “affine” analogs of designs is provided by the theory of matroids – or more precisely, of so-called perfect matroid designs in which all flats of same rank have equal cardinality. As it turns out there exist families of affine  $q$ -analog Steiner systems for several parameters. Besides being quite natural from a pure mathematical point of view, this approach is also viable for random network coding applications, when propagating in a network random affine combinations instead of linear ones, cf. [7].

Here is an outline of the paper. In Section 2 and Section 3 we provide an account of matroids and of finite geometry, as suitable for introducing the concept at hand. The discussion of projective and affine designs as well as their relationship then follows in Section 4. Finally, metric aspects and possible applications to the random network coding scenario are outlined in Section 5.

## 2. MATROIDS

The notion of a matroid was introduced by Whitney [15] as an abstraction of the concept of linear independence. It serves as a suitable framework for studying  $q$ -analogs of designs, as well as for developing metric and coding aspects in a general setting [7]. In this section we provide a brief treatment of some relevant aspects of matroid theory. For background reading and further details on matroids we refer to Oxley's monograph [13], while a concise introduction to designs in matroids can be found in [4].

**Definition 2.1.** A *matroid* is a pair  $(S, \mathcal{I})$ , where  $S$  is a finite set and  $\mathcal{I}$  is a nonempty family of subsets of  $S$  satisfying

- (i) if  $I \in \mathcal{I}$  and  $J \subseteq I$ , then  $J \in \mathcal{I}$ ;
- (ii) if  $I, J \in \mathcal{I}$  and  $|I| < |J|$ , there is  $x \in J \setminus I$  with  $I \cup \{x\} \in \mathcal{I}$  (*exchange axiom*).

A subset  $I$  of  $S$  is called *independent* if  $I \in \mathcal{I}$ , otherwise *dependent*.

**Examples 2.2.** The following are examples for matroids.

- (1) The *free matroid* is the matroid  $(S, \mathcal{P}(S))$ , where  $S$  is a finite set and  $\mathcal{P}(S)$  denotes the power set of  $S$ .
- (2) For a finite vector space  $V$ , the *vector matroid* is the matroid  $(V, \mathcal{I})$ , where  $\mathcal{I}$  is the family of all linearly independent subsets of  $V$ .
- (3) Let  $G = (V, E)$  be an undirected graph with finite vertex set  $V$  and edge set  $E \subseteq \binom{V}{2}$ . Then  $(E, \mathcal{I})$  is a *graphic matroid*, where a subset of the edges is independent if and only if it contains no cycle.

Given a matroid  $M = (S, \mathcal{I})$  and any subset  $X$  of  $S$  the *restriction*  $M|X := (X, \mathcal{I} \cap \mathcal{P}(X))$  is again a matroid. Finite restrictions of vector spaces or, equivalently, the column sets of matrices were among the original motivating examples of matroids, besides the graphic matroids.

In a matroid  $M = (S, \mathcal{I})$ , a maximal independent set is called a *basis*, and a minimal dependent set is a *circuit*. It follows from the exchange axiom that all bases have the same cardinality, and this number is called the *rank* of the matroid  $M$ . Moreover, the *rank*  $\rho(X)$  of a subset  $X$  of  $S$  is the rank of the restricted matroid  $M|X$ , i.e., the cardinality of a maximal independent subset of  $X$ .

**Proposition 2.3** (cf. [13, Cor. 1.3.4]). *The rank function  $\rho: \mathcal{P}(S) \rightarrow \mathbb{Z}$  of a matroid  $(S, \mathcal{I})$  satisfies the following properties for all subsets  $X, Y$  of  $S$ :*

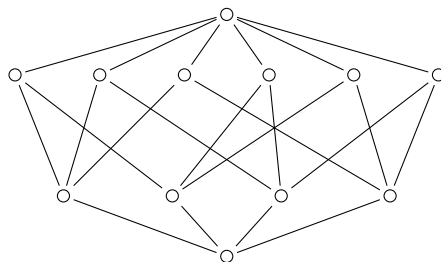
- (i)  $0 \leq \rho(X) \leq |X|$ ,
- (ii)  $X \subseteq Y$  implies  $\rho(X) \leq \rho(Y)$ ,
- (iii)  $\rho(X \cup Y) + \rho(X \cap Y) \leq \rho(X) + \rho(Y)$  (*submodular inequality*).

*Conversely, any mapping  $\rho: \mathcal{P}(S) \rightarrow \mathbb{Z}$  with these properties is the rank function of a matroid  $(S, \mathcal{I})$ , where  $\mathcal{I} := \{I \subseteq S \mid \rho(I) = |I|\}$ .*

The mapping  $\text{cl}: \mathcal{P}(S) \rightarrow \mathcal{P}(S)$  defined by

$$\text{cl}(X) := \{x \in S \mid \rho(X \cup \{x\}) = \rho(X)\}$$

for  $X \in \mathcal{P}(S)$  turns out to be a *closure operator*, i.e., it holds  $X \subseteq \text{cl}(X) = \text{cl}(\text{cl}(X))$  and  $\text{cl}(X) \subseteq \text{cl}(Y)$  if  $X \subseteq Y$ , for all  $X, Y \in \mathcal{P}(S)$ . A subset  $E$  of  $S$  satisfying  $E = \text{cl}(E)$  is called a *flat*, or a *k-flat* if its rank  $\rho(E)$  is  $k$ .

FIGURE 1. The lattice of the flats in  $\text{AG}(2,2)$ .

**Proposition 2.4** (cf. [13, Cor. 1.4.6]). *The closure operator  $\text{cl}: \mathcal{P}(S) \rightarrow \mathcal{P}(S)$  of a matroid  $(S, \mathcal{I})$  obeys the following for any flat  $E$  and any  $x, y \in S \setminus E$ :*

$$y \in \text{cl}(E \cup \{x\}) \text{ implies } x \in \text{cl}(E \cup \{y\}) \quad (\text{exchange property}).$$

*Conversely, any closure operator  $\text{cl}: \mathcal{P}(S) \rightarrow \mathcal{P}(S)$  with the exchange property is the closure operator of a matroid  $(S, \mathcal{I})$ , where  $\mathcal{I} := \{I \subseteq S \mid \forall x \in I : x \notin \text{cl}(S \setminus \{x\})\}$ .*

A subset  $X$  of  $S$  is called *generating* if  $\text{cl}(X) = S$ . It is easy to verify that the family of bases in a matroid coincides with the independent generating sets and also with the minimal generating sets.

**The lattice of flats.** For a matroid  $M = (S, \mathcal{I})$  let  $L(M) := \{E \subseteq S \mid \text{cl}(E) = E\}$  denote its collection of flats. When ordered by inclusion this is a *lattice*, i.e., for any flats  $E, F$  there exists a greatest lower bound or *meet*  $E \wedge F = E \cap F$  and a least upper bound or *join*  $E \vee F = \text{cl}(E \cup F)$ ; see Figure 1 for an example.

Notice that the rank function  $\rho: L(M) \rightarrow \mathbb{Z}$  on the set of flats is strictly isotone, i.e.,  $\rho(E) < \rho(F)$  if  $E \subsetneq F$ , as well as submodular, i.e.,  $\rho(E \vee F) + \rho(E \wedge F) \leq \rho(E) + \rho(F)$  for flats  $E, F$ . In this context the following result is of interest, which has been shown in a more general setup (see, e.g., [8, 12]). We include a direct proof for convenience (see also [7, Prop. 7, Cor. 2]).

**Proposition 2.5.** *In any lattice  $L$  with a strictly isotone and submodular function  $r: L \rightarrow \mathbb{R}$  a metric is given by  $d(x, y) := 2r(x \vee y) - r(x) - r(y)$ , for  $x, y \in L$ .*

*Proof.* The properties of a metric are clear, except for the triangle inequality. Let elements  $x, t, y \in L$  be given. Notice that

$$r(x \vee y) - r(x) \leq r(x \vee y \vee t) - r(x) = r(x \vee y \vee t) - r(x \vee t) + r(x \vee t) - r(x),$$

and the submodularity implies that

$$r(x \vee t \vee y) - r(x \vee t) \leq r(t \vee y) - r((x \vee t) \wedge (t \vee y)) \leq r(t \vee y) - r(t).$$

Hence  $r(x \vee y) - r(x) \leq r(x \vee t) - r(x) + r(t \vee y) - r(t)$ , and, by exchanging  $x$  and  $y$ , we get  $r(x \vee y) - r(y) \leq r(x \vee t) - r(t) + r(t \vee y) - r(y)$ . Adding these two inequalities we obtain  $d(x, y) \leq d(x, t) + d(t, y)$ , as desired.  $\square$

*Remark 2.6.* The same proof reveals that another metric on  $L$  is given by  $d'(x, y) := r(x \vee y) - \min(r(x), r(y))$ , for  $x, y \in L$ .

Accordingly, we associate for any matroid  $M$  on its set of flats  $L(M)$  the metric  $d_M(E, F) := 2\rho(E \vee F) - \rho(E) - \rho(F)$ , where  $E, F$  are flats.

We mention also the following characterization. Recall that in an ordered set an element  $y$  *covers* an element  $x$  if  $x < y$  but there is no element  $t$  such that  $x < t < y$ , and an *atom* is an element covering a least element. The lattice of flats is *atomistic*, i.e., every element is a join of atoms, as well as *semimodular*, i.e., if  $E$  and  $F$  both cover  $E \wedge F$ , then  $E \vee F$  covers both  $E$  and  $F$ ; consequently, the Jordan-Dedekind chain condition is satisfied, in fact, every maximal chain between flats  $E < F$  has length  $\rho(F) - \rho(E)$ . Conversely, every finite, atomistic and semimodular lattice can shown to be the lattice of flats in a matroid (cf. [13, Thm. 1.7.5]).

**Designs in matroids.** In order to define designs in matroids it is reasonable to restrict the class of matroids. A *perfect matroid design* (PMD) is a matroid  $M$  of some rank  $r$  for which any  $i$ -flat has the same cardinality  $f_i$ , where  $0 \leq i \leq r$ . In this case, we say that  $M$  is of *type*  $(f_0, \dots, f_r)$ .

**Examples 2.7.** The following are examples for perfect matroid designs.

- (1) The free matroid of rank  $n$ , i.e., the matroid  $(S, \mathcal{P}(S))$ , where  $S$  is a set of cardinality  $n$ , is a PMD with  $f_i = i$ , for  $0 \leq i \leq n$ .
- (2) For an  $n$ -dimensional vector space  $V$  over a finite field  $\mathbb{F}_q$ , the vector matroid  $(V, \mathcal{I})$  has rank  $n$  and its  $i$ -flats are the  $i$ -dimensional subspaces; it is a PMD with  $f_i = q^i$ , for  $0 \leq i \leq n$ .

A *loop* in a matroid  $(S, \mathcal{I})$  is an element  $x \in S$  such that  $\{x\} \notin \mathcal{I}$ . Two nonloops  $x, y \in S$  are *parallel* if  $\{x, y\} \notin \mathcal{I}$ . A matroid with no loops and no distinct parallel elements is called *geometric*. From any matroid one obtains a geometric matroid by deleting loops and identifying parallel elements. If  $M$  is a PMD of type  $(f_0, \dots, f_r)$ , then its geometrization is a PMD of type  $(f'_0, \dots, f'_r)$ , where  $f'_i := \frac{f_i - f_0}{f_1 - f_0}$ ; hence,  $f'_0 = 0$  and  $f'_1 = 1$ . In particular, the geometrization of a vector space over  $\mathbb{F}_q$  is the corresponding projective space, in which  $f_i = [i]_q := \frac{q^i - 1}{q - 1}$ .

**Definition 2.8.** Let  $M$  be a PMD of rank  $n$ . A  $t$ -( $n, k, \lambda$ ) *design* in  $M$  is a collection  $\mathcal{B}$  of  $k$ -flats in  $M$  such that each  $t$ -flat in  $M$  is contained in exactly  $\lambda$  members of  $\mathcal{B}$ .

For the free matroid  $M = (S, \mathcal{P}(S))$  one obtains the classical designs.

**Lemma 2.9.** Let  $M$  be a PMD of rank  $n$  and type  $(f_0, \dots, f_n)$ . Any  $t$ -( $n, k, \lambda$ ) design in  $M$  is also an  $s$ -( $n, k, \lambda_s$ ) design for  $s < t$ , where

$$\lambda_s = \lambda \prod_{i=s}^{t-1} \frac{f_n - f_i}{f_k - f_i}.$$

*Proof.* By induction it suffices to show the statement for  $s = t - 1$ , which follows by adapting the double-counting argument from the classical case. Let  $\mathcal{B}$  be a  $t$ -( $n, k, \lambda$ ) design, let  $E$  be any  $s$ -flat and consider all blocks  $B \in \mathcal{B}$  with  $E \subseteq B$ , the number being  $\lambda_s$ . Denoting, for  $B \in \mathcal{B}$  and  $x \in S$ ,  $\chi(x, B) = 1$  if  $x \in B$  and  $\chi(x, B) = 0$  otherwise, we have

$$\lambda_s(f_k - f_s) = \sum_{B, E \subseteq B} \sum_{x, x \notin E} \chi(x, B) = \sum_{x, x \notin E} \sum_{B, E \subseteq B} \chi(x, B) = (f_n - f_s)\lambda,$$

since if  $x \notin E \subseteq B$ , then  $x \in B$  if and only if  $\text{cl}(E \cup \{x\}) \subseteq B$ , which is a flat of rank  $s + 1 = t$ . Hence  $\lambda_s = \lambda \frac{f_n - f_s}{f_k - f_s}$ , independent of  $E$ , as desired.  $\square$

## 3. INCIDENCE GEOMETRY

The projective space and the affine space will provide natural classes of perfect matroid designs. We present here briefly the synthetic approach to these geometries, cf. [1, 2]. For simplicity all sets are assumed to be finite.

**Definition 3.1.** An *incidence space* is a triple  $\mathbf{G} = (\mathcal{P}, \mathcal{L}, I)$ , where  $\mathcal{P}$  and  $\mathcal{L}$  are sets, the elements of which are referred to as *points* and *lines*, respectively, and  $I \subseteq \mathcal{P} \times \mathcal{L}$  is a relation, called *incidence*, satisfying the following axioms:

- (i) for each pair of distinct points  $P$  and  $Q$  there is a unique line that is incident with  $P$  and  $Q$ , denoted by  $PQ$ ;
- (ii) each line is incident with at least two points.

For a point  $P$  and a line  $\ell$  with  $(P, \ell) \in I$  we say that  $P$  is incident with  $\ell$ ,  $P$  is on  $\ell$ ,  $\ell$  is incident with  $P$ , or  $\ell$  goes through  $P$ . Two lines  $\ell_1, \ell_2 \in \mathcal{L}$  *meet* if there is a point  $P$  on both  $\ell_1$  and  $\ell_2$ .

For a line  $\ell$ , denote by  $(\ell)$  the set of points incident with  $\ell$ . A set  $\mathcal{U}$  of points is called a *linear set* if  $(PQ) \subseteq \mathcal{U}$  for any distinct points  $P, Q$  of  $\mathcal{U}$ . Such a set defines an incidence space  $\mathbf{U} = (\mathcal{U}, \mathcal{L}', I')$  in a natural sense, called a *subspace* of  $\mathbf{G}$ . If the context is clear, we may identify a linear set and its corresponding subspace. The linear sets form a *closure system*, i.e., they are closed under arbitrary intersection. Given a subset  $\mathcal{X}$  of  $\mathcal{P}$  its *span*  $\text{cl}(\mathcal{X})$  is defined as the smallest linear set containing  $\mathcal{X}$ .

**Definition 3.2.** A *projective space* is an incidence space  $\mathbf{P} = (\mathcal{P}, \mathcal{L}, I)$  with the following properties:

- (i) if  $A, B, C, D$  are four points such that the lines  $AB$  and  $CD$  meet, then also the lines  $AC$  and  $BD$  meet (*Veblen-Young axiom*);
- (ii) each line is incident with at least three points.

It is easy to see that any subspace of a projective space is again a projective space. The family of all subspaces of a projective space with its natural incidence relation given by containedness is also called the *projective geometry*.

In any projective space the exchange property of the span holds, i.e., for any linear set  $\mathcal{U}$  and points  $P, Q \notin \mathcal{U}$  one has

$$Q \in \text{cl}(\mathcal{U} \cup \{P\}) \text{ implies } P \in \text{cl}(\mathcal{U} \cup \{Q\}).$$

Defining a set of points  $\mathcal{B}$  to be *independent* if  $P \notin \text{cl}(\mathcal{B} \setminus \{P\})$  for all  $P \in \mathcal{B}$ , then it follows from Proposition 2.4 that  $M_{\mathbf{P}} := (\mathcal{P}, \mathcal{I})$  is a matroid, where  $\mathcal{I}$  is the family of all independent sets.

An independent set  $\mathcal{B}$  that spans  $\mathcal{P}$  is called a *basis*. The cardinality of a basis  $\mathcal{B}$  is independent of its choice, and one defines  $\dim \mathbf{P} = |\mathcal{B}| - 1$  to be the *dimension* of  $\mathbf{P}$ . Accordingly, each linear subset  $\mathcal{U}$  is associated with a dimension, and one easily sees that a single point has dimension zero and a line dimension one; a two-dimensional subspace is called a *plane*, and a subspace of dimension  $\dim \mathbf{P} - 1$  is a *hyperplane*. We note that  $\dim \mathbf{P} = \rho(M_{\mathbf{P}}) - 1$ , where  $\rho$  is the matroid rank, and the  $k$ -flats are precisely the  $(k - 1)$ -dimensional subspaces.

**Definition 3.3.** An *affine space* is an incidence space  $\mathbf{A} = (\mathcal{P}, \mathcal{L}, I)$  such that the following axioms are satisfied:

- (i) there exists a *parallelism* on  $\mathbf{A}$ , i.e., an equivalence relation  $\parallel$  on  $\mathcal{L}$  such that for each point  $P$  and each line  $g$  there exists a unique line  $h$  through  $P$  such that  $h \parallel g$ , denoted by  $P \parallel g$ ;
- (ii) if  $A, B, C$  are noncollinear points and if  $A', B'$  are points with  $AB \parallel A'B'$ , then the lines  $A' \parallel AC$  and  $B' \parallel BC$  intersect in a point  $C'$  (*triangle axiom*).

Again, the span in affine space satisfies the exchange property. Thus the family of independent sets of an affine space  $\mathbf{A}$  form a matroid  $M_{\mathbf{A}}$ , and all bases have the same cardinality; the *dimension* of  $\mathbf{A}$  is  $\dim \mathbf{A} = |\mathcal{B}| - 1 = \rho(M_{\mathbf{A}}) - 1$ , where  $\mathcal{B}$  is a basis of  $\mathbf{A}$ .

There is a close relation between projective and affine spaces; in fact, every projective space induces an affine space and vice versa.

**Proposition 3.4.** Let  $\mathbf{P}$  be a projective space and  $\mathcal{H}$  a hyperplane in  $\mathbf{P}$ . Then  $\mathbf{A} = (\mathcal{P}', \mathcal{L}', I')$ , where  $\mathcal{P}' := \mathcal{P} \setminus \mathcal{H}$ ,  $\mathcal{L}' := \{\ell \in \mathcal{L} \mid \ell \not\subseteq \mathcal{H}\}$  and  $I' := I \cap (\mathcal{P}' \times \mathcal{L}')$ , defines an affine space.

**Proposition 3.5.** Let  $\mathbf{A} = (\mathcal{P}, \mathcal{L}, I)$  be an affine space. Let  $\mathcal{H} := \{[\ell] \mid \ell \in \mathcal{L}\}$ , where  $[\ell]$  denotes the parallel class of the line  $\ell$ . For  $\ell \in \mathcal{L}$  let  $\ell' := \ell \cup \{[\ell]\}$ , and for each plane  $\alpha$  in  $\mathbf{A}$  let  $\ell_\alpha := \{[\ell] \mid \ell \text{ line in } \alpha\}$ . Define

$$\mathcal{P}' := \mathcal{P} \cup \mathcal{H} \quad \text{and} \quad \mathcal{L}' := \{\ell' \mid \ell \in \mathcal{L}\} \cup \{\ell_\alpha \mid \alpha \text{ plane in } \mathbf{A}\}.$$

Then  $\mathbf{P} = (\mathcal{P}', \mathcal{L}', I')$  (with the obvious incidence) is a projective space in which  $\mathcal{H}$  is a hyperplane.

The cardinalities of subspaces in finite projective or affine spaces turn out to follow a regular pattern. A first result is that every line in a projective space  $\mathbf{P}$  is incident with the same number of points, and one calls  $q := |(\ell)| - 1 \geq 2$ , where  $\ell$  is a line, the *order* of  $\mathbf{P}$ .

**Theorem 3.6.** Any finite projective space of dimension  $d$  and order  $q$  has exactly  $q^d + \dots + 1 = \frac{q^{d+1}-1}{q-1}$  points. Therefore, each  $t$ -dimensional subspace has  $q^t + \dots + 1$  points.

Using the projective closure, one sees that all lines in a finite affine space  $\mathbf{A}$  have also the same number of points, and  $q := |(\ell)| \geq 2$ , where  $\ell$  is a line, is called the order of  $\mathbf{A}$ .

**Theorem 3.7.** Any finite affine space of dimension  $d$  and order  $q$  has exactly  $q^d$  points, and each  $t$ -dimensional subspace has  $q^t$  points.

As a consequence of Theorem 3.6 and Theorem 3.7 one sees that both in projective space and in affine space the matroid of independent sets is a perfect matroid design, and we can therefore define *projective* and *affine* designs using Definition 2.8.

**Coordinization.** Linear algebra provides a wealth of examples for projective spaces. Given a vector space  $V$ , let  $\mathbf{P}(V) := (\mathcal{P}, \mathcal{L}, I)$  be the incidence structure, where  $\mathcal{P}$  is the set of one-dimensional subspaces of  $V$ ,  $\mathcal{L}$  is the set of two-dimensional subspaces and the incidence  $I$  is given by containedness.

**Proposition 3.8.** *If  $V$  is an  $n$ -dimensional vector space over the finite field  $\mathbb{F}_q$ , then  $\mathbf{P}(V)$  is a projective space of dimension  $d := n - 1$  and order  $q$ , denoted by  $\text{PG}(d, q)$ . Its subspaces  $\mathbf{U}$  of dimension  $t := k - 1$  correspond to vector subspaces  $W \leq V$  of dimension  $k$ .*

Conversely, the first structure theorem for projective space implies the remarkable fact that any projective space  $\mathbf{P}$  of dimension  $\geq 3$  is of the form  $\mathbf{P}(V)$  for a vector space  $V$  over a (skew) field, cf. [2, Cor. 3.4.3].

For a vector space  $V$  one can also define the affine space  $\mathbf{A}(V) := (\mathcal{P}, \mathcal{L}, I)$ , where the points  $\mathcal{P}$  are (identified with) the vectors in  $V$ , the lines  $\mathcal{L}$  are the cosets of one-dimensional subspaces of  $V$  and the incidence  $I$  is given by containedness.

**Proposition 3.9.** *For a  $d$ -dimensional vector space  $V$  over  $\mathbb{F}_q$  the incidence structure  $\mathbf{A}(V)$  is an affine space of dimension  $d$  and order  $q$ , denoted by  $\text{AG}(d, q)$ . Its subspaces  $\mathbf{U}$  of dimension  $t$  are given by the cosets of  $t$ -dimensional subspaces of  $V$ .*

#### 4. DESIGNS IN FINITE GEOMETRIES

We are now prepared to state the definition of a projective design and of an affine design. Recall that in projective or affine space the (matroid) rank equals the geometric dimension plus one.

**Definition 4.1.** Let  $\mathbf{G} = (\mathcal{P}, \mathcal{L}, I)$  be a projective space or an affine space of rank  $n$  (dimension  $n - 1$ ). A  $t$ -( $n, k, \lambda$ ) *design* in  $\mathbf{G}$  is a collection  $\mathcal{B}$  of  $k$ -flats (i.e.,  $(k - 1)$ -dimensional subspaces) of  $\mathbf{G}$ , called *blocks*, such that every  $t$ -flat (i.e.,  $(t - 1)$ -dimensional subspace) of  $\mathbf{G}$  is contained in exactly  $\lambda$  blocks.

If  $\mathbf{G} = \mathbf{P}$  is a projective space we also refer to a  $t$ -( $n, k, \lambda$ ) *projective design*, and in case  $\mathbf{G} = \mathbf{A}$  is an affine space to an  $t$ -( $n, k, \lambda$ ) *affine design*. If  $\lambda = 1$  we speak of a (projective or affine) *Steiner system*  $S(t, k, n)$ .

Note that this definition is consistent with Definition 2.8 of designs in matroids. If the projective space is induced by a vector space we can translate Definition 4.1 into a more common form as follows. Let  $V$  be an  $n$ -dimensional vector space over  $\mathbb{F}_q$ , so that  $\mathbf{P}(V) = \text{PG}(n - 1, q)$ . A  $t$ -( $n, k, \lambda$ ) *subspace design* of order  $q$  is a collection  $\mathcal{B}$  of  $k$ -dimensional subspaces of  $V$  such that every  $t$ -dimensional subspace of  $V$  is contained in exactly  $\lambda$  members of  $\mathcal{B}$ .

**Affine designs from projective designs.** A *translation* of a vector space  $V$  is a map  $\alpha : V \rightarrow V$  of the form  $x \mapsto v + x$  for some  $v \in V$ . The set of all translations defines a group  $T$  under composition, which is isomorphic to  $V$  as an abelian group.

A nonempty subset  $W \subseteq V$  is an affine space if and only if  $W = \alpha U$  for some subspace  $U$  and a translation  $\alpha$ , i.e., if  $W = v + U$  for some  $v \in V$ . In this case,  $\dim U$  is the dimension of the affine space  $W$ . Note that an affine space is a vector subspace if and only if it contains  $0$ ; in fact, if  $0 \in \alpha U$ , then  $\alpha U = U$ .

**Theorem 4.2.** *Suppose that  $\mathcal{B}$  is a  $t$ -( $n, k, \lambda$ ) subspace design in  $V$ , then  $T\mathcal{B} := \{\alpha U \mid U \in \mathcal{B}, \alpha \in T\}$  is an  $(t+1)$ -( $n+1, k+1, \lambda$ ) affine design in  $\mathbf{A}(V)$ . Conversely, if  $\mathcal{D}$  is an  $(t+1)$ -( $n+1, k+1, \lambda$ ) affine design, then  $\mathcal{D}_0 := \{W \in \mathcal{D} \mid 0 \in W\}$  is a  $t$ -( $n, k, \lambda$ ) subspace design.*

*Proof.* We prove the latter statement first. All members  $W \in \mathcal{D}_0$  are  $k$ -dimensional subspaces. If  $X \leq V$  is any  $t$ -dimensional subspace, then  $X$  is also a  $t$ -dimensional

affine space. As  $0 \in X$ , clearly  $\{W \in \mathcal{D} \mid X \subseteq W\} = \{W \in \mathcal{D}_0 \mid X \subseteq W\}$  and by assumption the cardinality of this set is  $\lambda$ . This shows that  $\mathcal{D}_0$  is a  $t$ -( $n, k, \lambda$ ) subspace design.

Now consider the other statement. All members  $W \in T\mathcal{B}$  are certainly  $k$ -dimensional affine spaces. Let  $Y = \alpha X$  be any  $t$ -dimensional affine space, where  $X \leq V$  is a  $t$ -dimensional subspace and  $\alpha \in T$ . We claim that there is a bijection  $\{U \in \mathcal{B} \mid X \subseteq U\} \rightarrow \{W \in T\mathcal{B} \mid \alpha X \subseteq W\}$  given by  $U \mapsto \alpha U$ . Clearly,  $X \subseteq U$  implies  $\alpha X \subseteq \alpha U$ , thus the map is defined and obviously injective. On the other hand, if  $W = \beta U \in T\mathcal{B}$  satisfies  $\alpha X \subseteq \beta U$ , then  $0 \in X \subseteq \alpha^{-1}\beta U$  and hence  $\alpha^{-1}\beta U = U$ ; thus  $W = \beta U = \alpha U$  and  $X \subseteq U$ , which shows surjectivity. Therefore, the sets have the same cardinality  $\lambda$ , which shows that  $T\mathcal{B}$  is an affine design.  $\square$

**Proposition 4.3.** *For any 2-( $n, k, \lambda$ ) subspace design there is a 2-([ $n$ ] $_q$ , [ $k$ ] $_q$ ,  $\lambda$ ) classical design, where [ $d$ ] $_q := \frac{q^d - 1}{q - 1}$ . For any 2-( $n, k, \lambda$ ) affine design there is a 2-( $q^{n-1}, q^{k-1}, \lambda$ ) classical design, and for any 3-( $n, k, \lambda$ ) affine design of order  $q = 2$  there is a 3-( $2^{n-1}, 2^{k-1}, \lambda$ ) classical design.*

*Proof.* For the subspace design, let  $V$  be an  $n$ -dimensional vector space and consider the points  $\mathcal{P}$  of its projective space  $\mathbf{P}(V)$ , i.e., the set of all its one-dimensional subspaces; thus  $|\mathcal{P}| = [n]_q$ . Each block  $U$  of a 2-( $n, k, \lambda$ ) subspace design corresponds to a subset  $\mathcal{U} := \{P \in \mathcal{P} \mid P \subseteq U\}$  of cardinality  $[k]_q$ , and a two-element set  $\{P, Q\}$  of  $\mathcal{P}$  is contained in such a set  $\mathcal{U}$  if and only if the two-dimensional subspace spanned by  $P$  and  $Q$  is contained in a block  $U$ . Thus any 2-set of  $\mathcal{P}$  is contained in exactly  $\lambda$  blocks.

Now let  $V$  be a vector space of dimension  $n - 1$  and consider a design in  $\mathbf{A}(V)$  consisting of  $(k - 1)$ -dimensional affine spaces. Then  $V$  has  $q^{n-1}$  elements, each block has  $q^{k-1}$  elements, and a block contains a two-element set  $X$  if and only if it contains the affine space (a line) generated by  $X$ . This shows the claim for 2-( $n, k, \lambda$ ) affine designs.

Finally, if the ground field of the vector space  $V$  is  $\mathbb{F}_2$ , then any three points are affine independent, i.e., they span a two-dimensional affine space (a plane). As three points are in a block if and only if their generated plane is contained in the block, the last claim follows.  $\square$

By combining Theorem 4.2 and Proposition 4.3 we immediately get:

**Corollary 4.4** (cf. [6, Th. 4]). *For any 2-( $n, k, \lambda$ ) subspace design of order 2 there is a 3-( $2^n, 2^k, \lambda$ ) classical design. In particular, for any  $S(2, 3, n)$  subspace Steiner system one obtains a classical  $S(3, 8, 2^n)$  Steiner system.*

**Existence of affine Steiner systems.** Recall that a *spread* in a projective geometry  $\mathbf{P}$  of rank  $n$  (dimension  $n - 1$ ) is a projective Steiner system  $S(1, k, n)$ , i.e., a partition of the point set of  $\mathbf{P}$  into subspaces of rank  $k$  (dimension  $k - 1$ ). It is well-known that for any order  $q$  a spread exists if and only if  $k \mid n$  (cf. [5, p29]). Therefore, Theorem 4.2 readily implies the following result.

**Proposition 4.5.** *For any  $k, \ell$  there is an affine Steiner system  $S(2, k + 1, k\ell + 1)$ .*

This shows, of course, for any order  $q$  and for all  $\ell$  the existence of Steiner triple systems  $S(2, 3, 2\ell + 1)$  in affine geometry, and in particular the “affine  $q$ -analog” of the Fano plane  $S(2, 3, 7)$ .



**Example 4.6.** Consider an affine Steiner system  $S(2, 3, 7)$  for  $q = 2$ . This is a family  $\mathcal{B}$  of planes in  $\mathbf{A}(\mathbb{F}_2^6)$  such that each line is contained in exactly one plane in  $\mathcal{B}$ . As there are 2016 lines in  $\mathbf{A}(\mathbb{F}_2^6)$  the size of  $\mathcal{B}$  is  $\frac{1}{6} \cdot 2016 = 16 \cdot 21 = 336$ .

Note that the affine Steiner system  $S(2, 3, 7)$  constructed from a spread  $S(1, 2, 6)$  in  $\text{PG}(5, 2)$  cannot be extended to a subspace code in the Grassmannian  $\mathcal{G}_2(7, 3)$  of minimum distance 4 (i.e., to a partial projective Steiner system). Indeed, this affine Steiner system  $S(2, 3, 7)$  features only 21 parallel classes, while the projective closures of parallel planes will intersect in a common line at infinity.

In this context we mention that there is a different affine Steiner system  $S(2, 3, 7)$ , which is invariant under the Singer cycle of size 63 and which has 273 parallel classes. It has been used in [6, Lem. 6] to construct a covering code in  $\mathcal{G}_2(7, 3)$  of size 399, covering the 2-dimensional subspaces.

**Question 4.7.** Does there exist an affine Steiner system  $S(2, 3, 7)$  for  $q = 2$ , which is *skew*, i.e., with no pair of parallel planes? If yes, then a new subspace code in  $\mathcal{G}_2(7, 3)$  of distance 4 and size 336 is found, improving on the largest size 333 of such a code reported so far [9]. If no, then the long-standing open problem on the existence of the projective  $q$ -analog of the Fano plane  $S(2, 3, 7)$  (of size 381) would be settled, as such a structure cannot exist in this case.

## 5. RANDOM NETWORK CODING

In this final section we discuss possible applications of affine designs in a random network coding scenario. It is straightforward to adapt the concept of random network coding [10] for affine spaces, by stipulating that the inner nodes in a non-coherent network forward a random *affine* combination of the incoming symbols, instead of a linear combination. That is, if  $v_1, \dots, v_s \in V$  are the received vectors on the incoming edges of a node, the output along any outgoing edge is an affine combination  $\sum_{i=1}^s \lambda_i v_i$ , where the coefficients  $\lambda_i$  are randomly chosen such that  $\sum_{i=1}^s \lambda_i = 1$ , i.e.,  $\lambda_s = 1 - \sum_{i=1}^{s-1} \lambda_i$ . This is detailed and analyzed in [7], where it is shown that affine network coding saves about one symbol when compared to the standard linear network coding approach.

Regarding error-correction it is customary in coding theory to use a metric space in order to model the distance between the sent and the possibly altered received codeword. We consider thus metrics in geometries and related concepts below.

Let  $\mathbf{G}$  be a projective or an affine geometry of rank  $n$ , i.e., of dimension  $n - 1$ . Then, as noted after Proposition 2.5, a metric on its set of flats is given by

$$d(E, F) := 2r(E \vee F) - r(E) - r(F),$$

where  $E, F$  are flats and  $r$  denotes the (matroid) rank. A *small-intersection code* or a *partial  $S(t, k, n)$  Steiner system* in  $\mathbf{G}$  is a collection  $\mathcal{C}$  of  $k$ -flats such that  $r(E \cap F) < t$  for all distinct flats  $E, F \in \mathcal{C}$ . Clearly, if an  $S(t, k, n)$  Steiner system exists it is a small-intersection code of maximal cardinality.

In projective geometry the *modular equality*  $r(E \vee F) + r(E \wedge F) = r(E) + r(F)$  holds, and thus we can write for the matroid metric

$$d(E, F) = r(E \vee F) + r(E \wedge F) = r(E) + r(F) - 2r(E \wedge F),$$

which for  $\mathbf{G} = \mathbf{P}(V)$  equals the subspace distance of the corresponding subspaces in  $V$ . In this case, a small-intersection code is just a code  $\mathcal{C}$  in the Grassmannian

$\mathcal{G}(n, k)$  of minimum distance  $d(\mathcal{C}) \geq 2(k - t + 1)$ , and is usually simply referred to as a *subspace code*.

On the other hand, in affine geometry the modular equality does not hold. In fact, the formula

$$d_{\wedge}(E, F) := r(E) + r(F) - 2r(E \wedge F)$$

does not define a metric, as the triangle inequality is not satisfied in general. For example, if  $E, F$  are parallel planes and  $T$  is a further plane that intersects both  $E$  and  $F$  in a line, then  $d_{\wedge}(E, F) = 6$ , but  $d_{\wedge}(E, T) + d_{\wedge}(T, F) = 2 + 2 = 4$ .

**Recovery of deletions.** Notwithstanding the above remark, small-intersection codes in affine geometry (and thus affine Steiner systems) are interesting in a network coding scenario for the correction of *deletions*, i.e., in a situation when during transmission no erroneous vectors are being injected into the network, but some information may be lost due to lack of connectivity.

The abstract framework for adversarial error correction of [14, Sec. III] can be applied in the present situation. Let  $L$  be the lattice of flats in an affine (or a projective) geometry. Define the *deletion discrepancy*  $\Delta : L \times L \rightarrow \mathbb{N} \cup \{\infty\}$  by

$$\Delta(E, F) := \begin{cases} r(E) - r(F) & \text{if } F \subseteq E, \\ \infty & \text{otherwise.} \end{cases}$$

The following result is immediate from [14, Prop. 1].

**Proposition 5.1.** *A code  $\mathcal{C} \subseteq L$  is  $e$ -deletions-correcting if  $e \leq \min_{E \neq E' \in \mathcal{C}} \tau(E, E')$ , where  $\tau(E, E') = \min_{F \in L} \max\{\Delta(E, F), \Delta(E', F)\} - 1$ .*

In particular, if  $\mathcal{C}$  is a small-intersection-code with parameters  $(t, k, n)$ , then  $\tau(E, E') = k - r(E \cap E') - 1 \geq k - t$  for any distinct  $E, E' \in \mathcal{C}$ . Hence such a code is able to correct up to  $e = k - t$  deletions, i.e., when up to  $k - t$  independent vectors less than submitted are obtained by the receiver.

**A polynomial-based code construction.** In affine geometry, a construction of good codes with respect to the metric  $d$  has been proposed based on a lifting of maximum rank-distance codes [7]. Here we present some good small-intersection codes, which follow the construction of subspace codes based on linearized polynomials [11] and allow for a slightly wider range of parameters.

Recall that a *linearized polynomial* is a polynomial  $f \in \mathbb{F}_{q^m}[X]$  of the form  $f = f_0X + f_1X^q + \dots + f_rX^{q^r}$  for some  $f_i \in \mathbb{F}_{q^m}$ ; these are exactly the polynomials  $f$  (of degree  $< q^m$ ), for which the associated map  $\mathbb{F}_{q^m} \rightarrow \mathbb{F}_{q^m}$ ,  $x \mapsto f(x)$ , is  $\mathbb{F}_q$ -linear. An *affine polynomial* is a polynomial  $g \in \mathbb{F}_{q^m}[X]$  of the form  $g = a + f$  with  $a \in \mathbb{F}_{q^m}$  and a linearized polynomial  $f \in \mathbb{F}_{q^m}[X]$ ; these are the polynomials  $g$  such that their corresponding function is  $\mathbb{F}_q$ -affine, i.e.,  $g(\lambda x + \mu y) = \lambda g(x) + \mu g(y)$  for  $x, y \in \mathbb{F}_{q^m}$  and  $\lambda, \mu \in \mathbb{F}_q$  with  $\lambda + \mu = 1$ .

For  $t \geq 1$  let  $\mathcal{L}_t := \{a + \sum_{i=0}^{t-2} f_i X^{q^i} \mid a, f_i \in \mathbb{F}_{q^m}\}$  be the set of affine polynomials up to degree  $q^{t-2}$ . Let  $t - 1 \leq \ell \leq m$  and let  $U$  be an  $\mathbb{F}_q$ -affine subspace of  $\mathbb{F}_{q^m}$  of dimension  $\ell$ . Define

$$\mathcal{C} := \{\Gamma(g|_U) \mid g \in \mathcal{L}_t\},$$

where  $\Gamma(g|_U) \subseteq U \times \mathbb{F}_{q^m}$  denotes the graph of  $g|_U : U \rightarrow \mathbb{F}_{q^m}$ ,  $x \mapsto g(x)$ .

**Proposition 5.2.** *The code  $\mathcal{C}$  has  $q^{mt}$  elements and is a partial  $S(t, k, n)$  Steiner system in  $\mathbf{A}(V)$ , where  $V := U \times \mathbb{F}_{q^m}$  and  $n := r(V) = \ell + m + 1$ ,  $k := r(X) = \ell + 1$  and  $r(X \cap Y) < t$  for distinct  $X, Y \in \mathcal{C}$ .*

*Proof.* For different polynomials  $g, h \in \mathcal{L}_t$ , due to the maximum degree the functions  $g|_U$  and  $h|_U$  coincide on at most  $q^{t-2} < q^\ell$  elements, which shows that  $X = \Gamma(g|_U)$  and  $Y = \Gamma(h|_U)$  are distinct and  $r(X \cap Y) = \dim(X \cap Y) + 1 \leq t - 1$ . Then the rest is clear.  $\square$

**Example 5.3.** Let  $q = 2$ . Considering, say,  $m = \ell = 3$  and  $t = 3$  we get from Proposition 5.2 a small-intersection code in  $\text{AG}(6, q)$ , which is a partial  $S(3, 4, 7)$  Steiner system with  $q^9 = 512$  elements. For  $t = 2$  we obtain accordingly a partial  $S(2, 4, 7)$  Steiner system with  $q^6 = 64$  elements, and by Proposition 4.5 there is even a full  $S(2, 4, 7)$  Steiner system, which has 72 elements.

Comparing the codes with their siblings in projective geometry, one sees from [9] that the best subspace codes with these parameters have fewer elements, namely  $A_2(n, d; k) = A_2(7, 4; 4) = A_2(7, 4; 3) \leq 381$  and  $A_2(7, 6; 4) = A_2(7, 6; 3) = 17$ .

#### ACKNOWLEDGMENTS

The author would like to thank Stefan E. Schmidt and Anna-Lena Horlemann-Trautmann for helpful discussions, and gratefully acknowledges continuous support from COST Action IC1104 “Random Network Coding and Designs over  $\text{GF}(q)$ ”.

#### REFERENCES

- [1] M. K. Bennett, *Affine and projective geometry*, John Wiley & Sons, Inc., New York (1995)
- [2] A. Beutelspacher, U. Rosenbaum, *Projective geometry: from foundations to applications*, Cambridge University Press, Cambridge (1998)
- [3] M. Braun, T. Etzion, P. Östergård, A. Vardy, A. Wassermann, “Existence of  $q$ -analogs of Steiner systems,” Preprint, arXiv:1304.1462 (2013), 10 pages.
- [4] P. J. Cameron, M. Deza, “Designs and matroids,” in: C. J. Colbourn, J. H. Dinitz (eds.), *Handbook of Combinatorial Designs*, CRC Press (2006), 847–852.
- [5] P. Dembowski, *Finite geometries*, Springer-Verlag, Berlin-New York (1968)
- [6] T. Etzion, A. Vardy, “On  $q$ -analogs of Steiner systems and covering designs,” *Adv. Math. Commun.* **5**(2) (2011), 161–176.
- [7] M. Gadouleau, A. Goupil, “A matroid framework for noncoherent random network communications,” *IEEE Trans. Inf. Theory* **57**(2) (2011), 1031–1045.
- [8] L. Haskins, S. Gudder, “Height on posets and graphs,” *Discr. Math.* **2**(4) (1972), 357–382.
- [9] D. Heinlein, M. Kiermaier, S. Kurz, A. Wassermann, “Tables of subspace codes,” Preprint, arXiv:1601.02864 (2016), 13 pages. <http://subspacecodes.uni-bayreuth.de>
- [10] T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi, B. Leong, “A random linear network coding approach to multicast,” *IEEE Trans. Inf. Theory* **52**(10) (2006), 4413–4430.
- [11] R. Koetter, F. R. Kschischang, “Coding for errors and erasures in random network coding,” *IEEE Trans. Inf. Theory* **54**(8) (2008), 3579–3591.
- [12] B. Monjardet, “Caractérisations métriques des ensembles ordonnés semi-modulaires,” *Math. Sci. Hum.* **56**(8) (1977), 77–87.
- [13] J. Oxley, *Matroid theory*, Second Ed., Oxford University Press, Oxford, 2011.
- [14] D. Silva, F. R. Kschischang, “On metrics for error correction in network coding,” *IEEE Trans. Inf. Theory* **55**(12) (2009), 5479–5490.
- [15] H. Whitney, “On the abstract properties of linear dependence,” *Amer. J. Math.* **57**(3) (1935), 509–533.